GROUP-IB

INTELLIGENCE INSIGHTS.

Middle East, Türkiye & Africa

December

INTRODUCTION

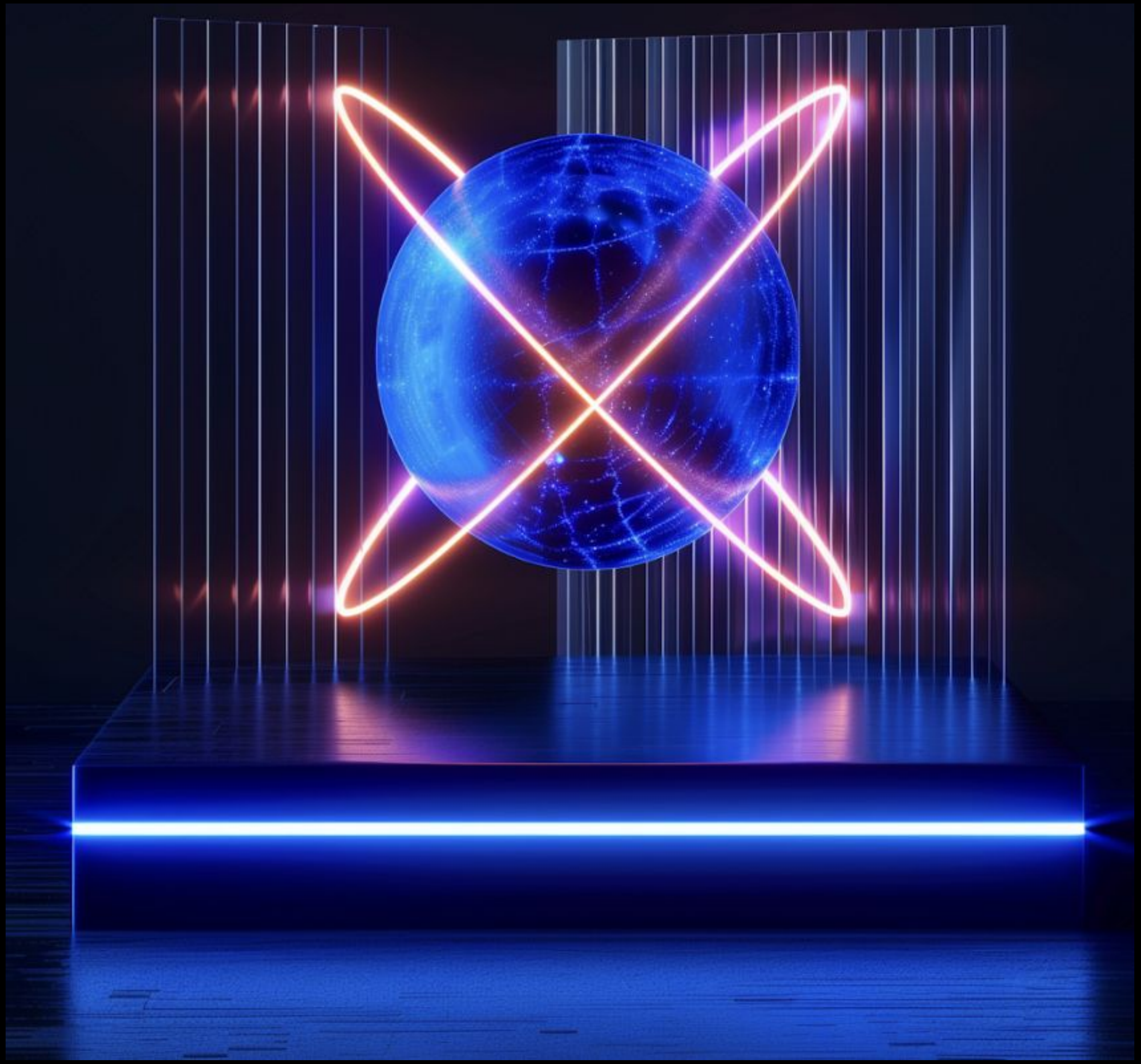
This report contains information on the most significant cybersecurity events that occurred worldwide and in the META region over the last month.

2 notable events of the month:

→ **Group-IB published a blogpost where discusses how smartphone manufacturers often conceal security flaws, posing significant risks to users and businesses.**

→ **Group-IB observes an increase in the use of compromised accounts of legitimate organizations by the group MuddyWater in their campaigns.**

Group-IB specialists discovered multiple phishing and scam campaigns and took active steps to negate their disruptive impact. We want to highlight that **Group-IB customers are well-protected** and aware about such types of threats.



GLOBAL TRENDS

Global trends with a brief description:

01 Group-IB published blogpost with brief overview of exploitation vulnerabilities in mobile OSes.

The blog post "Patch Me If You Can: The Truth About Smartphone Vulnerabilities" by Group-IB discusses how smartphone manufacturers often conceal security flaws, posing significant risks to users and businesses. It emphasizes the importance of timely updates and provides actionable steps to protect devices from data breaches, identity theft, and exploitative attacks.

02 Group-IB published report about abusing Deepfake technology in fraud campaigns.

Group-IB's Fraud Protection team reports that fraudsters are increasingly using deepfake technology to bypass biometric security measures, such as facial recognition and liveness detection, in financial institutions. Techniques include the use of emulators, app cloning, and virtual cameras to exploit system vulnerabilities, posing significant financial and societal risks.

03 Group-IB performed in-depth research of multiples Fake reCAPTCHA campaigns.

The ClickFix infection chain operates at its core by deceiving users into taking an action to continue internet browsing. Pup-ups are shown with dialog requiring the user to press on buttons like "Fix It", "I am not a robot", etc… Once clicked, a malicious powershell script is automatically copied to the user's clipboard. Users are deceived into pasting the script into the RUN dialog after pressing Windows key + R, thereby executing the malware without their knowledge. This technique facilitates the infection process, enabling attackers to deploy malware with direct help of users.

REGIONAL TRENDS

Key regional trends with a brief description:

01 Group-IB observes an increase in the usage of compromised accounts of legitimate organizations by the group MuddyWater in their campaigns.

National-state MuddyWater APT group actively uses compromised emails by putting them into RMM config files. Discovered emails were not previously detected in any leakages- this may indicate that the account was directly compromised by the group.

Middle East, Türkiye and Africa

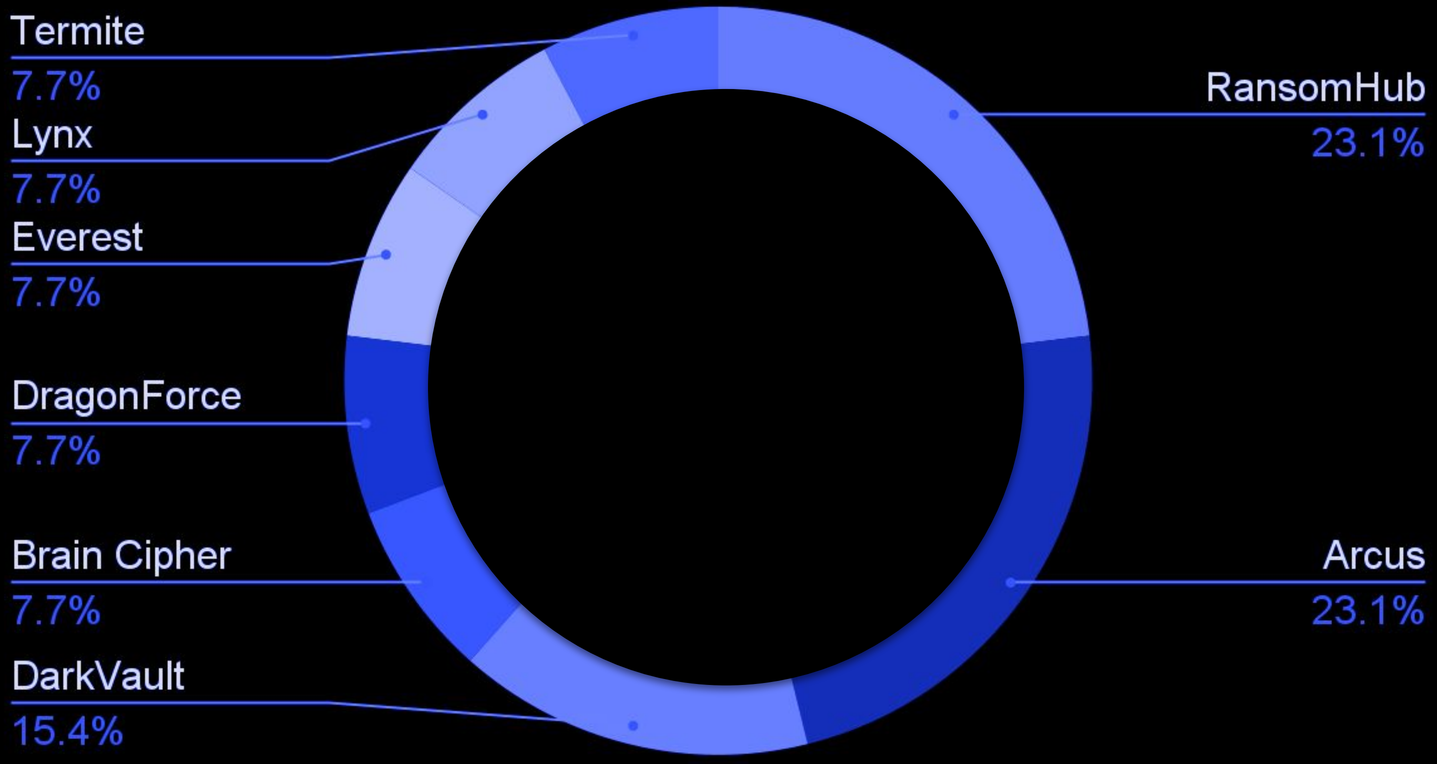
STATISTICS: **ATTACKS**

GROUP-IB

RANSOMWARE ACTIVITIES

Ransomware is a type of malicious software that encrypts the victim's data, rendering it inaccessible. The attacker then demands a ransom payment from the victim to restore access to the data, typically threatening to delete or publicly expose the data if the ransom is not paid. Ransomware statistics for the last month in META region:

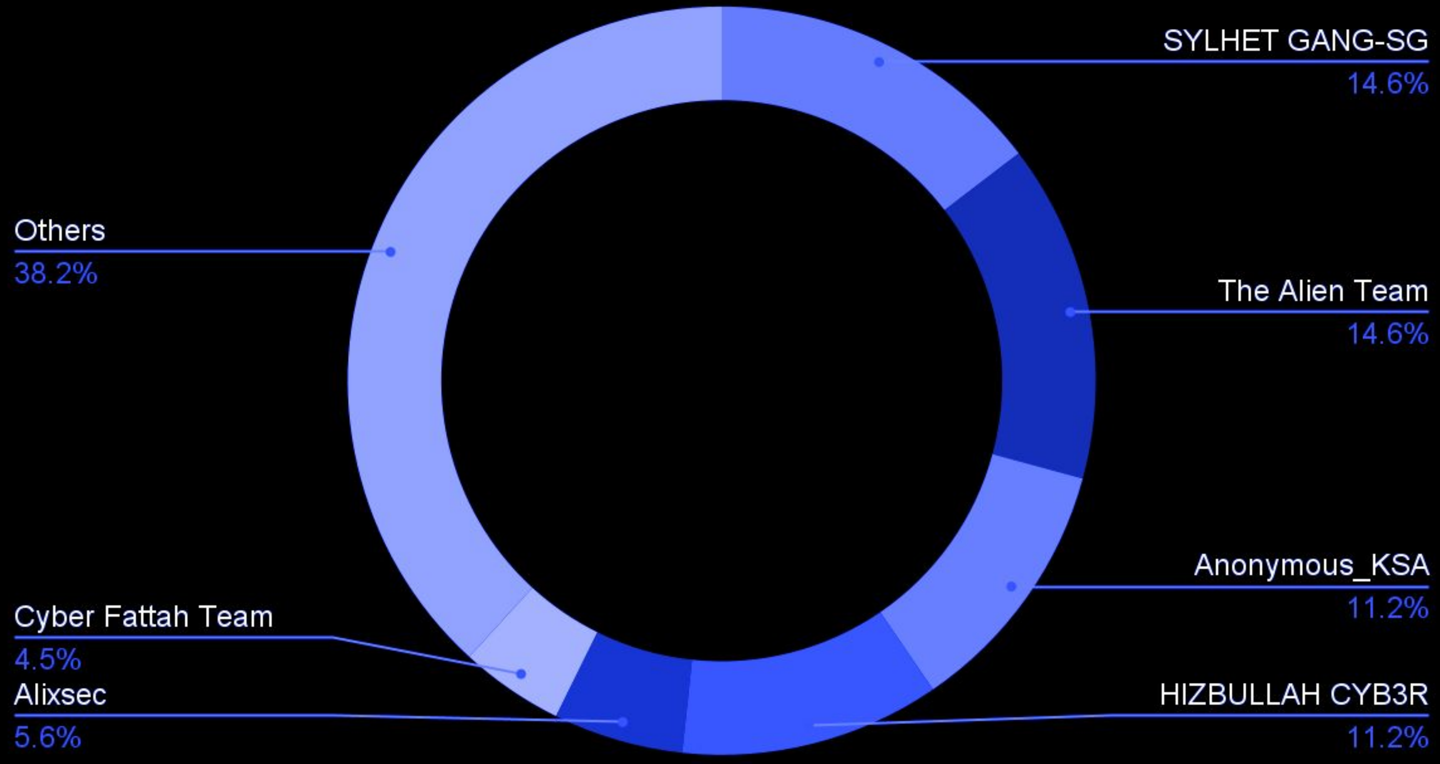
RANSOMWARE Attacks per Group



HACKTIVISM ACTIVITIES

Hacktivism is the use of hacking to promote political or social agendas. Usually hacktivist groups are low-skill hackers who perform DDoS, Defacement, and Data Breaches (mostly leverages compromised accounts) attacks. Unfortunately, during the last year these groups attracted a lot of attention. Below is a brief overview of groups that were active in the region during the previous month.

HACKTIVISM Attacks per group

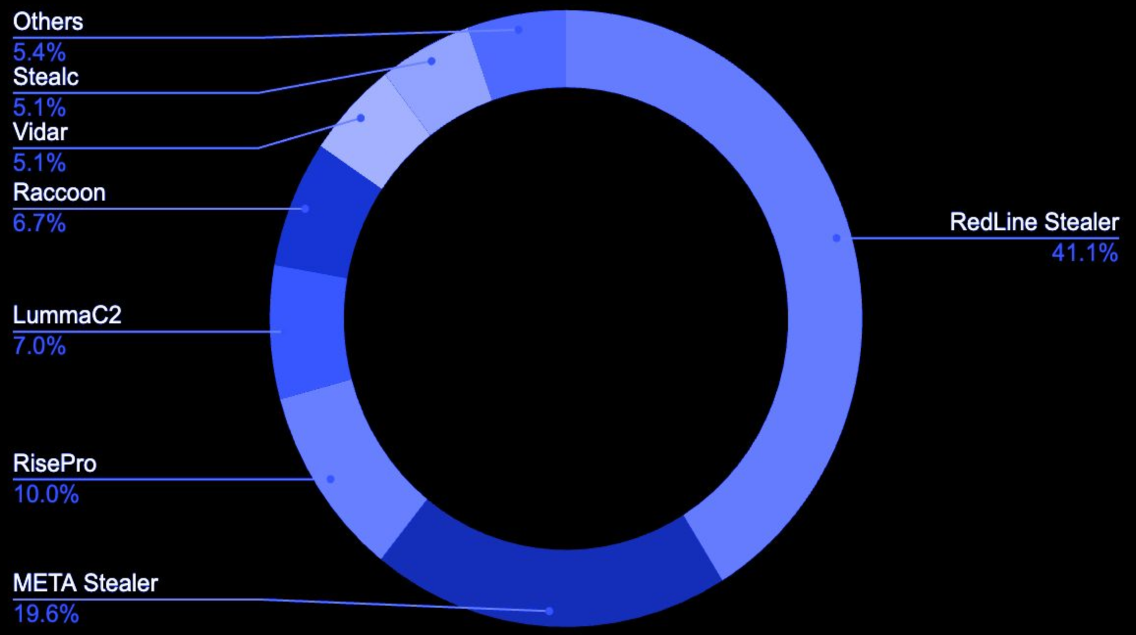


STATISTICS: **COMPROMISED DATA**

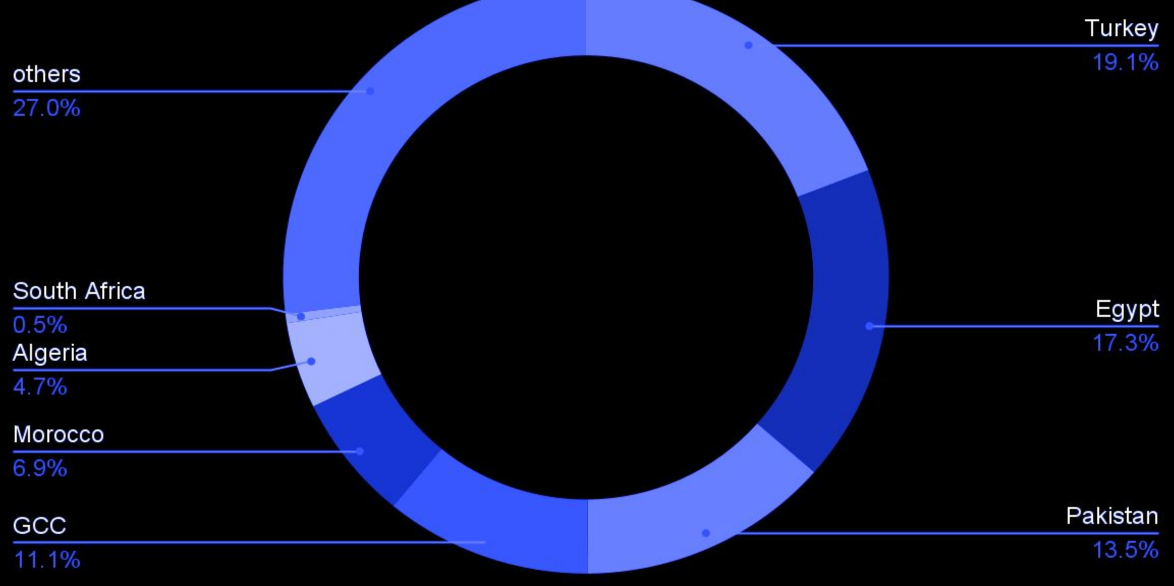
Compromised accounts are a significant threat because they allow unauthorized access to sensitive personal or corporate information, leading to potential financial loss, identity theft, and reputational damage. Additionally, compromised accounts can be used to launch further attacks, causing operational disruptions and exposing organizations to legal and regulatory consequences.

In this part of the report, we provide statistics regarding compromised accounts and compromised cards — all to understand which malware families are the most active in the region.

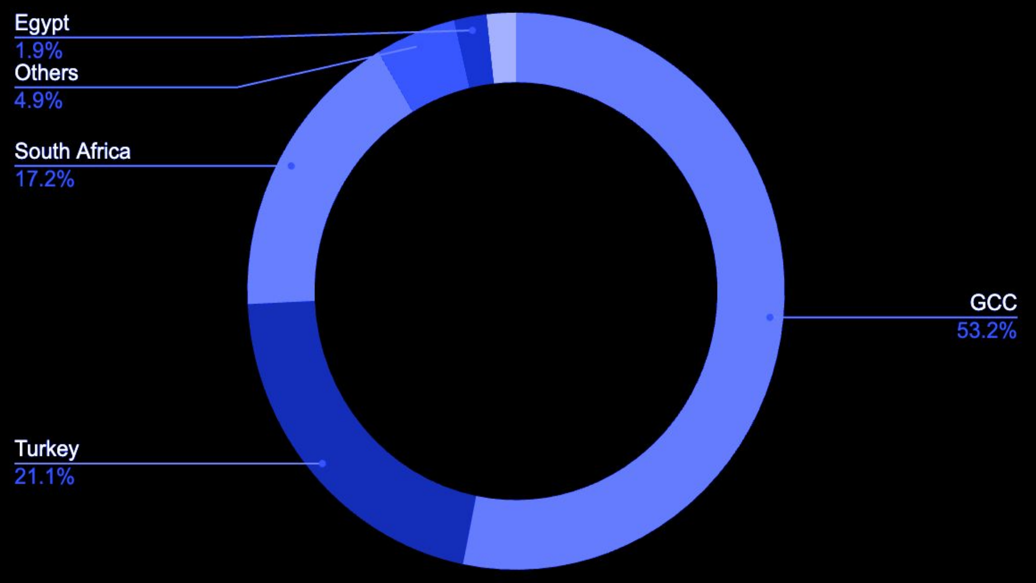
Compromised data by Malware



Compromised accounts by country



Compromised Bank Cards by Country



CONCLUSIONS AND RECOMMENDATIONS

GROUP-IB

The evolving threat landscape poses significant risks to organizations across various sectors. The incidents discussed in this report underscore the need for upgraded security measures and proactive threat management. To safeguard your organization, consider implementing the following recommendations:

ENHANCE SECURITY AWARENESS TRAINING

Regularly educate employees on recognizing phishing attempts, social engineering tactics, and safe online practices.

STRENGTHEN IT INFRASTRUCTURE

Ensure all systems are updated with the latest security patches and employ multi-factor authentication (MFA) to enhance access controls.

CONDUCT REGULAR SECURITY AUDITS

Perform periodic assessments of your IT environment to identify and mitigate potential vulnerabilities.

DEPLOY ADVANCED THREAT DETECTION TOOLS

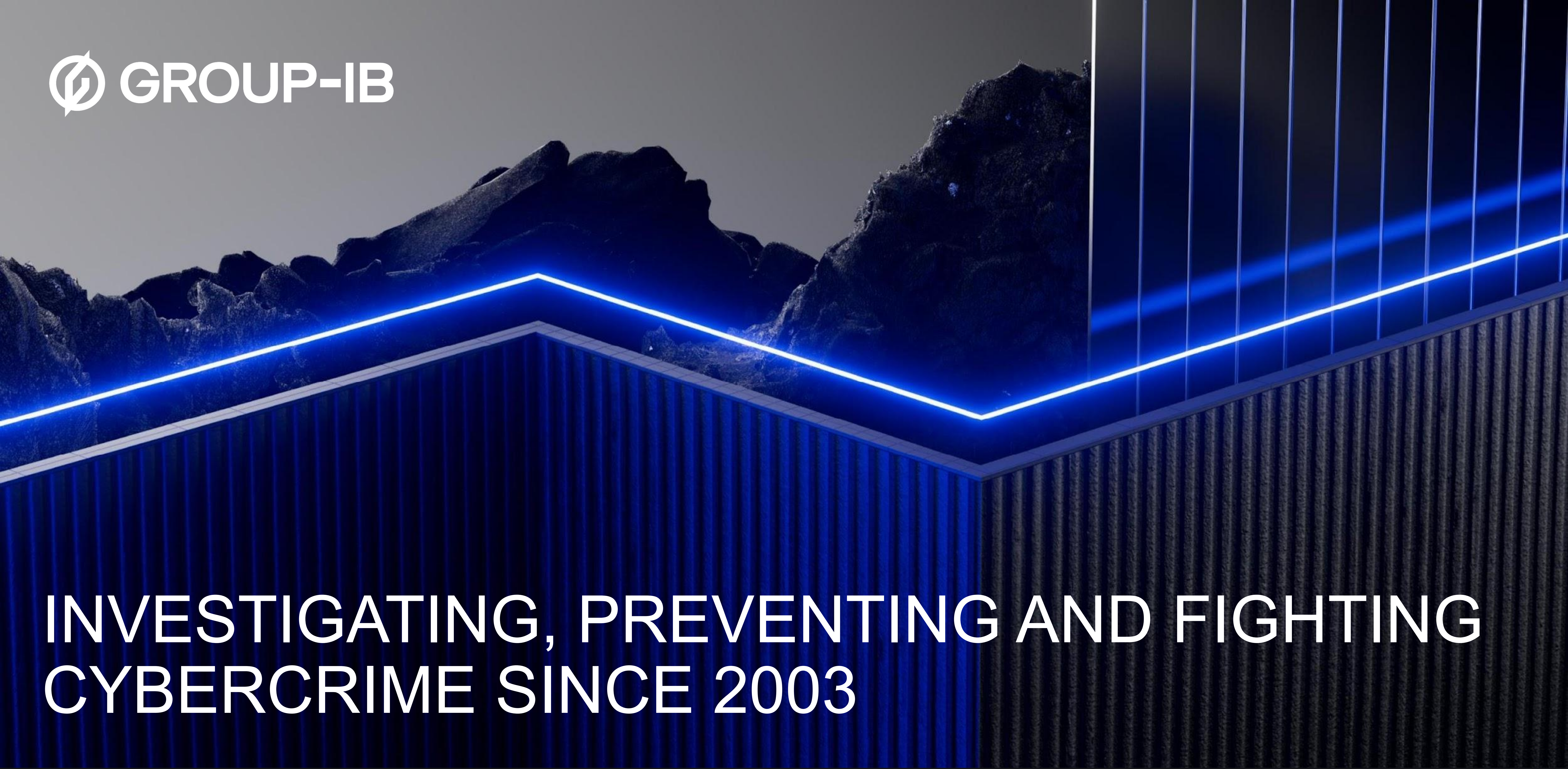
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

ESTABLISH INCIDENT RESPONSE PROTOCOLS

Develop and regularly update an incident response plan to quickly address and mitigate the impact of security breaches.

COLLABORATE WITH THREAT INTELLIGENCE SERVICES

Leverage threat intelligence services to stay informed about emerging threats and adjust your security strategies accordingly.



GROUP-IB

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM

GROUP-IB.COM/BLOG
+971 45681785

LINKEDIN FACEBOOK TWITTER INSTAGRAM